Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 15-29

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

A Secured Clinic Booking System using Multi-Factor Authentication

Maisarah Jaafar[1], Isredza Rahmi A Hamid[1]*

[1]Faculty of Computer science & Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, Malaysia

DOI: https://doi.org/10.30880/aitcs.2023.04.02.002
Received 06 November 2023; Accepted 06 Noember 2023; Available online 30 November 2023

Abstract: Online Booking system is a software platform where user do not use phone tag and emails to book their sessions. Phone tag is a scenario where two parties contacted each other by telephone calls or messages. Dr. Hannani Clinic's existing system implements the online booking system. However, the systems did not have proper security mechanisms to authenticate the user. The proposed Secured Clinic Booking system allows patients to book their appointment online with multi-factor authentication. We apply multi-factor authentication that consists of strong password, security question and Completely Automated Public Turing to test Computer and Human Apart (CAPTCHA). This project uses an object-oriented approach and hypertext preprocessor (PHP) programming language. The proposed system can secure the clinic booking system. Thus, the integrity of the online booking information is protected.

Keywords: Online Clinic, Booking System, Security Mechanism, Multi-factor authentication, Object-Oriented Approach, Data Breach

1. Introduction

In the last few years, most of the clinics managed and recorded their patient and appointment data manually by using paper based. Since the pandemic of Covid-19, all processes have shifted to online because the number of patients increased, and they must follow standard operating procedure (SOP). However not all online systems apply a proper authentication technique. Online booking is a software platform that allows customers to choose their date and time without using phone tags and email [1]. Sometimes the patients cannot attend the appointment due to busy schedule.

Dr. Hannani Clinic used an online clinic booking system. The booking system provides a convenient appointment scheduling system that allow patients to book the appointment anytime. Patients need to choose the services, doctor and time that have been provided. After patient choose the booking session, they need to enter their details such as full name, phone number and email. However, there are no security mechanisms implemented in this system to authenticate the user. This will give an

*Corresponding author: rahmi@uthm.edu.my

opportunity for attacker to attack the system and get user's personal data. Other than that, clinics might possibly get fake appointments requests that wasted doctor's time and prevent others from booking the appointment. Therefore, this threat can be reduced by implementing multi-factor authentication to ensure that only the authorized user can access the system.

Multi-factor authentication is developed to improve the security layer of the system that requires two or more different factors to authenticate the user. The multi-factor authentication that implemented in this system are password, security question and CAPTCHA. Multi-factor authentication is a user-friendly and reliable authentication when accessing the system [3]. Even though the system has been hardened, the attacker will always find a way to get access to the system illegally.

There are three types of users that can access in the proposed system which are patient, doctor, and clinic assistant. The new user is only for patients and doctors while nurse is an admin who managed the system. To access the system, the new user must register their name, ID number, address, phone number, email and password. Then, they must enter the username, password and verify the CAPTCHA to login the system. Users need to verify CAPTCHA by entering random characters before clicking on login button. Only valid input data is allowed. Each of the users has their own modules and functions that can be accessed. Passwords for each user will be hashed using AES encryption algorithm.

The objectives of this project are to design a clinic booking system using multifactor authentication, to develop a secure booking system with multi-factor authentication using password, security question and CAPTCHA and to test the functionality of the proposed system in terms of user acceptance and system functionality. The rest of the paper is organized as follows: Section 2 discusses the related work of the clinic booking system. Then, Section 3 describes the methodology that has been used in this paper and section 4 discusses system analysis and design and section 5 discusses the conclusion of the proposed system.

2. Literature Review

This section explains about the literature review that has been done related to the online booking system, authentication approach and existing online booking system.

2.1 Online Booking System

Online booking system is an eHealth healthcare facility that has been revolutionized by Information and Communication Technology (ICT) [5]. Online booking system used scheduling algorithm to help patients book their session without using phone tags and email. The manual booking method is used manual method to record and arrange the appointment schedule and \required admin to check the appointment date regularly and reschedule if there are any changes happened [6]. Due to this, sometimes patients need to wait for a long time waiting for their sessions. Thus, an online booking system is introduced to reduce the extended waiting time for both doctor and patient and allow patient to book their appointment session anytime.

2.2 Authentication Approach

Authentication is a process where a system will verify a user's identity by using a set of identifying credentials. It is also a process which will validate the authenticate user before enabling them to access the protected system. Authentication always occurs at the start of the application and acts as a permission before allowed user to proceed. Then, the system will determine if a user's credentials match with database, then it proves that it is an authorized user [7]. The authentication approaches are strong password, Completely Automated Public Turing test to tell Computers and Human Apart (CAPTCHA), security question, barcode, and Radio Frequency Identification (RFID).

2.2.1 Password

A password is a secret word or code that functions as a security measure to prevent any unauthorized access to the protected data [8]. The strong password describes a password that humans and computer program or bots find difficult to guess as it must consist of a least eight characters, have combination of uppercase and lowercase, a mixture of letters and numbers and have at least one special character [9]. It is important to protect the system from any brute-force attack and password-hacking techniques.

2.2.2 Completely Automated Public Turing test to tell Computers and Human Apart (CAPTCHA)

CAPTCHA is a type of security measure that consists of randomly generated sequence of letters and/or numbers and clicking a text box says, "I'm not a robot". This kind of test only can be completed by human and not bots because bots find difficult to understand the language [10]. CAPTCHA is designed to protect the system from any spamming ads that promote scams that may contain a virus and protect from email worms or junk emails [11].

2.2.3 Security Question

Security question is a secret form that requires the patient to choose and answer the question. It typically involves asking the user to provide an answer to a personal question such as favorite genre movie, favorite sports during primary school, that is only known by the user. The answer is then compared to the answer in database and if it matches, the user is granted access to a secure system or an account. Security question has been implemented in this system because it is as secure as you make them. It means that the more difficult the question the more difficult the attacker is to find the answer.

2.2.4 Radio Frequency Identification (RFID)

RFID is a technology of wireless communication that uses radio waves frequency to automatically identify the object and collect data from them. It is a process where RFID tags and antenna are used to send the data to RFID reader to convert the radio frequency into usable data. RFID tag is safer than barcode because the RFID will not require individual to make a direct contact and avoid from any damages like ripping and smearing [15].

2.2.5 Biometric

Biometric authentication is a security method where the process of identifying and authenticating by looking at unique biological characteristics of individual [13]. This method is a process of comparing the physical and behavior traits to be stored in a database. Authentication is validated when both samples of biometric data match. There are some common biological characteristics that are used as biometric authentication such as voice recognition, fingerprint scanning, facial recognition, iris recognition and heart rate sensors.

2.3 Existing Booking System

This section discusses the existing systems which is similar to the proposed secure booking system. The existing systems are Airasia flight booking system, Eatigo.com restaurant booking system and Golden Screen Cinema (GSC) Ticket movie booking system.

2.3.1 Airasia Flight Booking System

In Airasia flight booking system, users can simply access the system by signing up their email and password or use Google, Facebook, or WeChat accounts. The system also suggested password or user can use their own password. For login button, the system verifies the user where they need to enter the phone number and One-Time Password (OTP) will be sent through SMS.

2.3.2 Eatigo.com Restaurant Booking System

Eatigo.com is one of the foods reservations systems that used by many restaurants in Malaysia. Eatigo.com allows customers to reserve their sits by entering their name, email, and phone number. Customers can choose the time and number of people for dining. Then, the reservation details will be sent through the customer's email. If customers want to enjoy their special deals, they need to register and log into the websites. They use SHA-1 hashed to hash user's credentials.

2.3.3 Golden Screen Cinema (GSC) Ticket Booking System

Movie ticket booking system is a web-based application where customers reserve their ticket and seats, and the system is available 24/7 to customer book anytime. Golden Screen Cinema (GSC) is a cinema that provides an online ticket booking system. First, the customer needs to choose the movie, the available date and time with their preferable seats. The number of seats defined the number tickets they want to buy. If a customer already has an account, they need to enter their phone number and password. If they do not have an account, they need to sign up with their name, phone number, TAC number, email, and password. This system used Two-Factor Authentication that is available in this system which are password and One-Time Password (OTP). OTP is a code that contain4 random numbers and can be sent to email.

2.4 Comparison Between Existing System and Proposed System

Table 1 shows the comparison between existing booking systems which are flight booking system, restaurant reservation system and movie ticket booking system with the proposed system which is secure clinic booking system. The features included login and sign up, multi factor authentication, database used, authentication approach, encryption algorithm and programming language used.

Table 1: Comparison between similar system with proposed system

Features	Airasia Flight Booking System	Eatigo.com Restaurant Booking System	GSC Ticket Booking System	Proposed System
Login / Sign Up page	Yes	Yes	Yes	Yes
Multifactor Authentication	No	No	No	Yes
Database Used	Yes	No	No	Yes
Authentication Approach	Password, OTP	Password	Password, OTP	Password, CAPTCHA, security question
Encryption Algorithm	Advanced Encryption Standard (AES)	SHA-1	Not Encrypted	Advance Encryption Standard (AES)
Programming Language	JavaScript	Not Stated	JavaScript	PHP

Both Airasia and GSC system use the same authentication approach which are password and OTP number. OTP number will automatically send by the system to the user's SMS to authenticate the user while Eatigo.com only used password for authentication approach and has higher possibility for attacker to do Brute-Force Attack, meanwhile the authentication approaches for proposed system are password, CAPTCHA and security question.

Moreover, Airasia and the proposed system used Advanced Encryption Standard (AES) method to encrypt the data while Eatigo.com used SHA-1 encryption method. Meanwhile, the encryption method used by GSC system is not stated. And last, Airasia and GSC system used Javascript programming language, proposed system used PHP programming language and Eatigo.com system is not stated.

3. Methodology

This section discussed the methodology that was used in this project. Object-Oriented Methodology (OOM) implemented by using an agile model. The Agile model consists of four phases which are system analysis, system design, object design and implementation phase as shown in Figure 1.

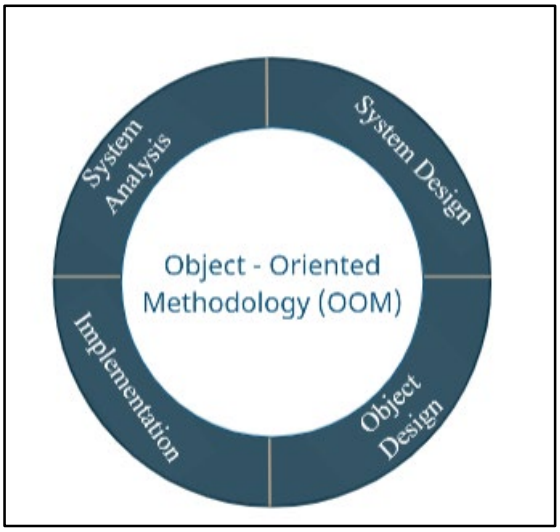

Figure 1: Object-Oriented Methodology (OOM) [14]

Based on the develop system, in the system analysis, the data was collected from the existing company. The interview was carried out with the admin of Dr Hannani clinic. There were 25 questions that asked the admin that related with online appointment booking system include login, register, booking and database.

Next, in the system design phase, all the architecture design includes data flow diagram (DFD), activity diagram, flowchart to represent the process involved during developing the system. In addition, a data dictionary has also been created.

In the object design phase, a complete architecture for the proposed system is designed. For Dr. Hannani online clinic booking system, there are eight tables for entity-relationship diagram. Entity-relationship diagram is a database table that shows the connection between the entity involved. The table includes patients, booking service, doctor, schedule, nurse, and appointment details.

Object-oriented implementation and testing are the last phase where the system will be tested and its functionality will be defined. In this phase, all the database and classes must link together to make sure that the system will produce the expected output. The system will call from the database and ensure that all the called are accurate and available.

4. Analysis and Design

This section explains the design of the system which consists of functional and non-functional requirements, system analysis and system design.

4.1 Functional Requirement

Functional requirement defines a function of a module or component of the system as shown in Table 2. It is to describe when user input the desired requirements, whether the system produces an expected output or not.

Table 2: Functional Requirements of the system

Module	Functionalities
Register	
- Patient	- User register as a new user to the system
- Doctor	- The details include password will be stored in the database.
Login	
- Patient	- User inputs valid password, CAPTCHA
- Admin	- System will popup alert if any invalid input
- Doctor	- Users verify by entering correct security questions and answer.
Booking appointment	- Patient book appointment
- Patient	- Booking appointment only valid for available data, time, services, and doctor's schedule
Schedule Arrangement	- Only nurses can manage the schedule.
- Admin	- The unavailable date, time and doctor in charge must not work if user click.
	- Avoid from redundancy
Add Doctor	
- Admin	- Only admin be able to add and delete the doctor
Delete patient and doctor.	
- Admin	- Only admin can delete patient and doctor

4.2 Non-Functional Requirements

Non-functional requirement defines the attributes of the system. It includes the aspects that will ensure the usability and functionality of the system. Table 3 shows the non-functional requirement in the proposed system.

Table 3: Non-Functional Requirements

Modules	Functionalities
Usability	- System should show the right page depends on the user's access
Security	- Password is encrypted by using AES encryption algorithm.
	- The password must be alphanumeric.
	- The answer to security question must match with database.
Availability	- The system only works if internet connection is available

4.3 System Analysis

System analysis is the first process to propose the existing system. This section discusses Unified Modelling Language (UML). Unified Modelling Language (UML) is a standardized modelling language which involves a set of notation graphics that describes the flow of the system. Figure 2 shows the modules that can be accessed by the patient. There are five modules include login and register, appointment booking, insert OTP to confirm the booking, update profile and logout module. Patients need to register by entering their name, IC number, email, phone number, address, and password. Then, they must verify their IC number, password, and CAPTCHA to login to the system. In addition, they need to choose the security question and answer it correctly.

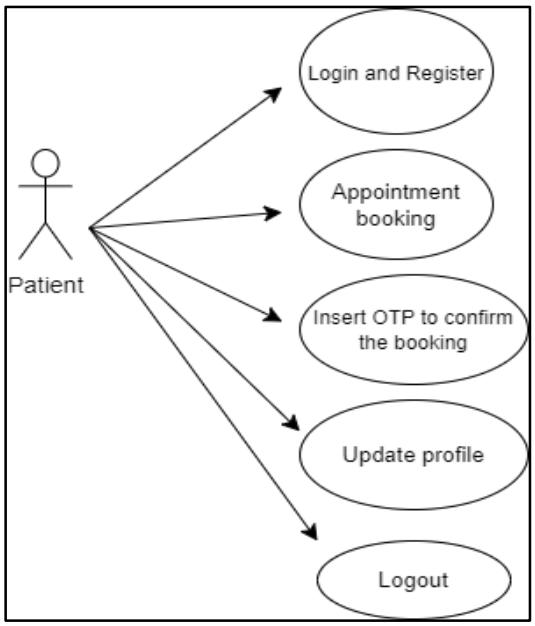

Figure 2: Patient use case

Figure 3 shows a use-case for doctors. There are four modules that doctors can access in the system which include login, view patient and schedule, view patient details, update profile and logout. Doctors can straightforwardly login by using the default password that has been set by the admin. However, doctors can update their password and personal details in a user profile tab.

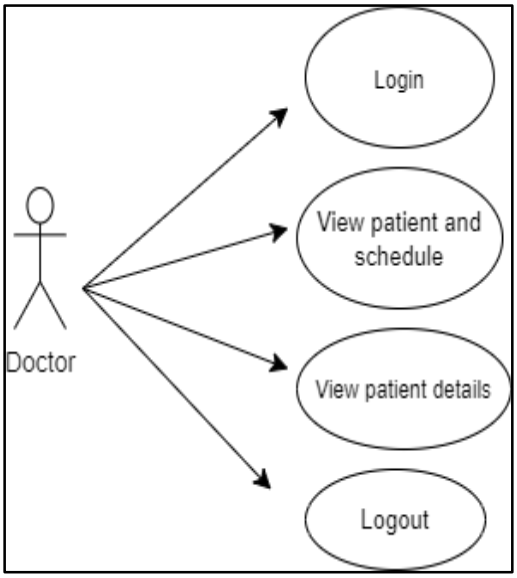

Figure 3: Doctor use case

Figure 4 shows the use-case for admin. There are five modules that admin can access which are login, manage schedule, add doctor, view appointment details, and delete user, view audit trail and logout. Admin is the only person who can manage the system; thus, they just need to login and no register is needed. Admin can add a doctor and manage doctor's schedule.

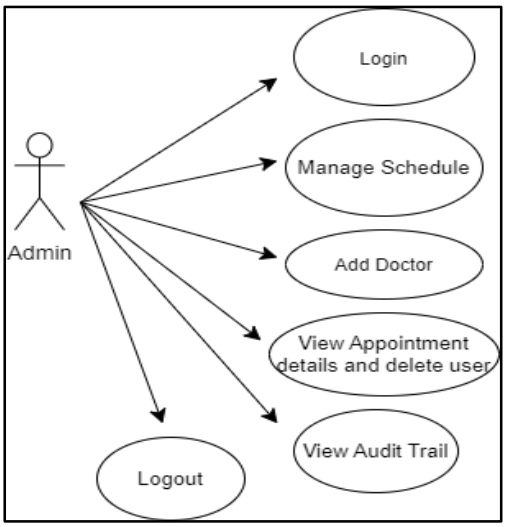

Figure 4: Admin use case

4.4 System Design

This section explains the system architecture design and flowchart.

4.4.1 System Architecture Design

System architecture is a conceptual model that defines the behavior of the system to achieve the objective. Figure 5 shows the system architecture design for the proposed system. This system uses a web-based user interface to allow patients, doctors, and nurses to manage and access the modules. The modules include login, register, booking appointment, manage schedule, approve, and delete user, view schedule and view appointment details.

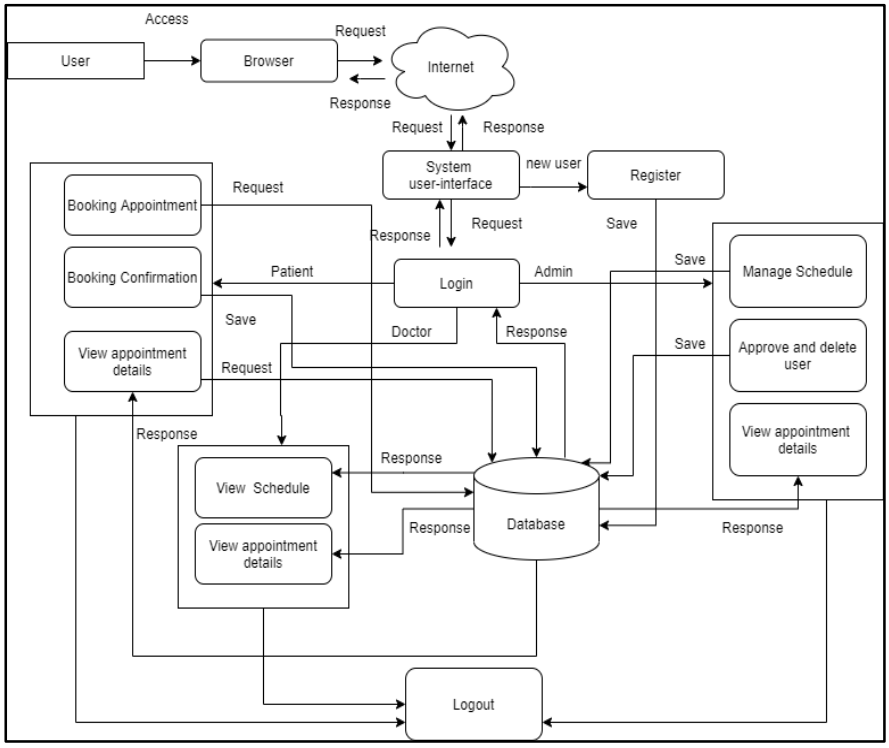

Figure 5: System Architecture Design

4.4.2 Flowchart

Flowchart is a simple algorithm that represents different with different function that connect by arrow. The combination of the shapes shows the flow and process of the system. It helps to simplify the complex process and ease the stakeholders to understand the proposed system. Hence, flowchart can explain about the data insert, the expected output and the modules involved. Figure 6 shows the flowchart for the proposed system that describes all the processes involving patient, admin and doctor.

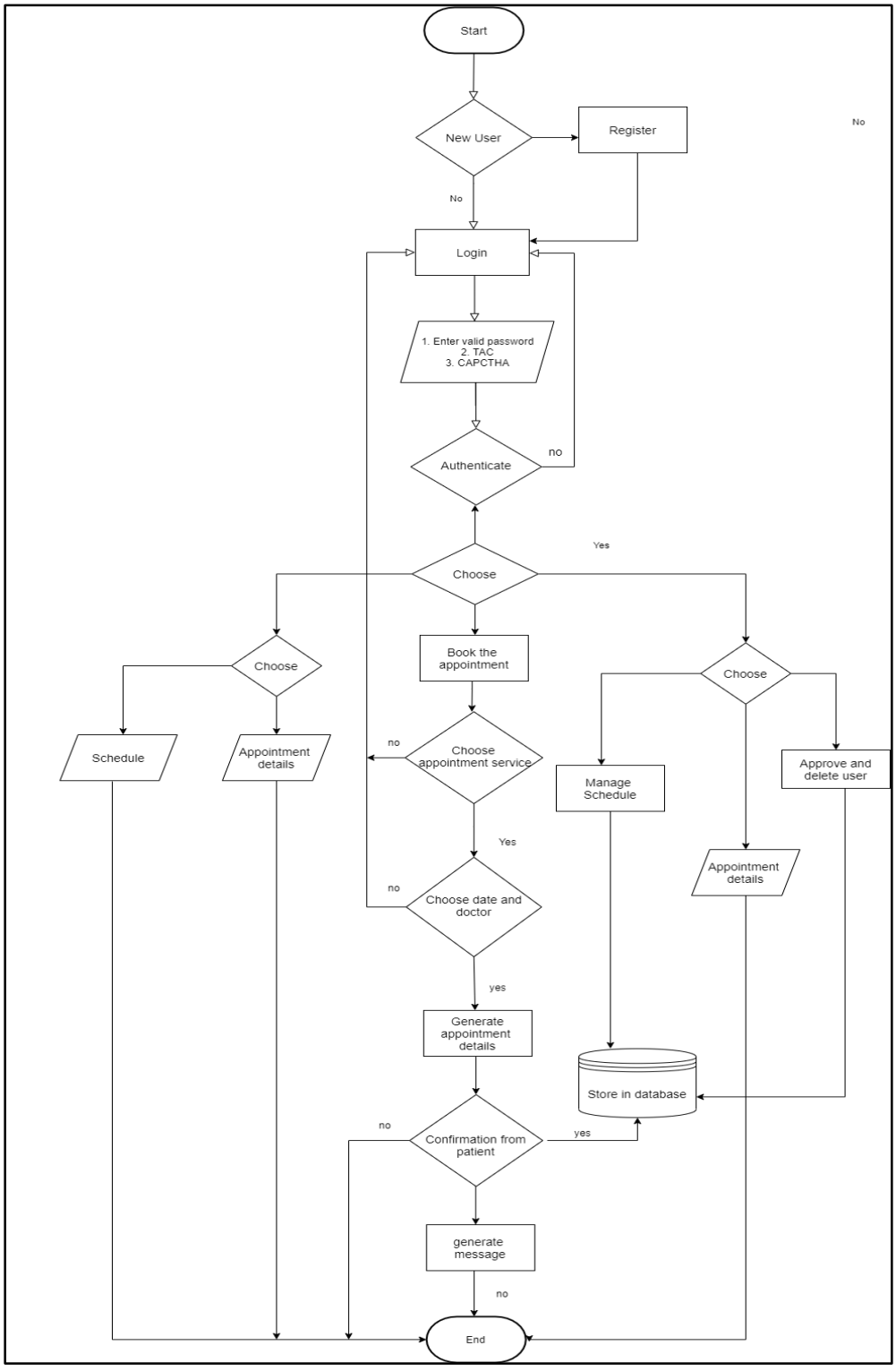

Figure 6: Flowchart of the proposed system

4.5 Object Design

In this phase, a complete architecture for the clinic booking system is designed.

4.5.1 Entity-Relationship Diagram

Figure 7 shows the entity-relationship diagram (ERD) which explains the attributes and the data that are being created, used, and stored in the database according to the proposed system. There are eight tables for entity-relationship diagram. Entity-relationship diagram is a database table that shows the connection between the entity involved. The tables include patients, booking service, doctor, schedule, nurse, and appointment details. All the database table includes primary and foreign key.

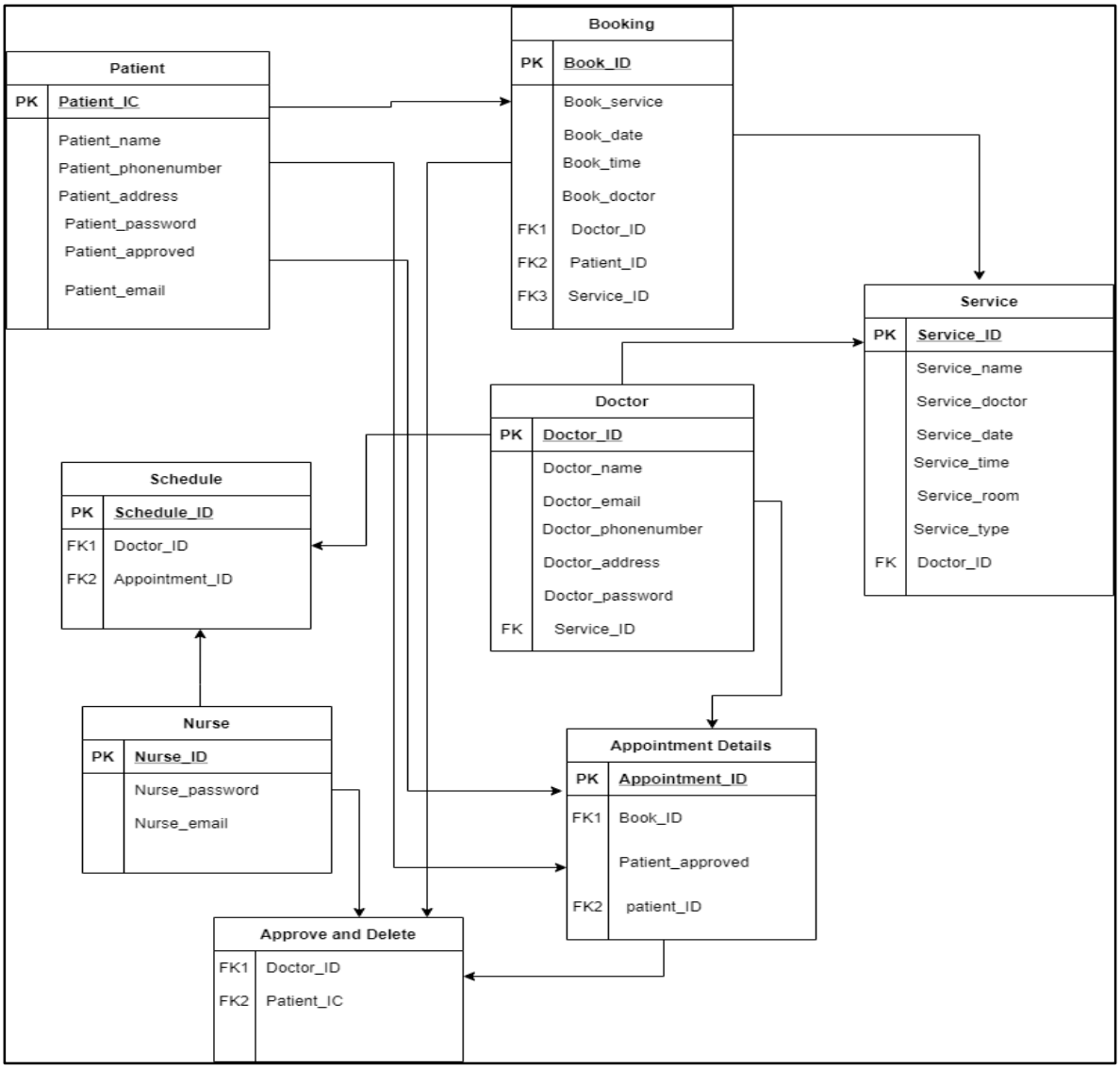

Figure 7: Entity Relationship Diagram

4.6 Implementation

Implementation and testing are the last phase where the system will be tested, and its functionality will be defined.

4.6.1 Registration and Login page.

Figure 8 shows the login page design for the proposed system. There are four requirements which include username, password and verify CAPTCHA. Figure 9 shows the verification page designed for

the patients. Users need to enter their name, email, phone number, address, and alphanumeric password to register for the system. Next, patients need to enter their identification card, correct password, and verify the CAPTCHA as shown in Figure 10. Then the patient will be redirected to verification page, and they need to choose security question, and answer it correctly. If the input is correct, then the patient can proceed to book their appointment.

Figure 8: Login page interface

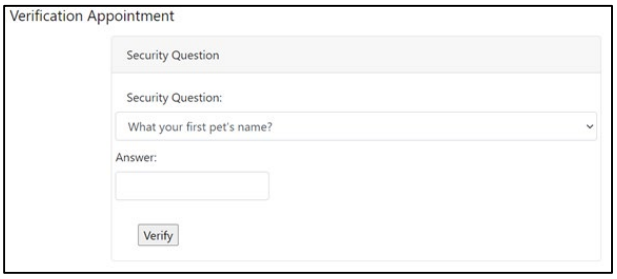

Figure 9: Verification page for patient

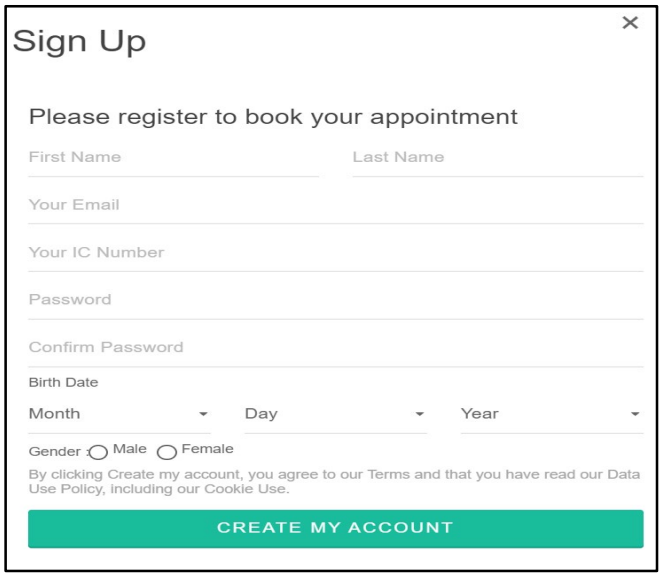

Figure 10: Registration page interface

4.6.2 Booking Appointment

Before a patient book their appointment session, they need to choose the available date, slots and doctor that will be redirected after the login process. Figure 11 shows the appointment interface that patients need to choose the appropriate date and click on the 'Book now' button to proceed their appointment.

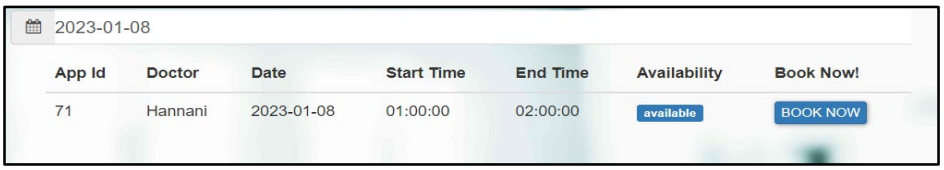

Figure 11: Booking appointment interface

4.6.3 Update profile Interface

Patients and doctors can update their profile in the profile user tab. Figure 12 shows the updated profile interface. They cannot update their IC number because the IC number is used as a primary key.

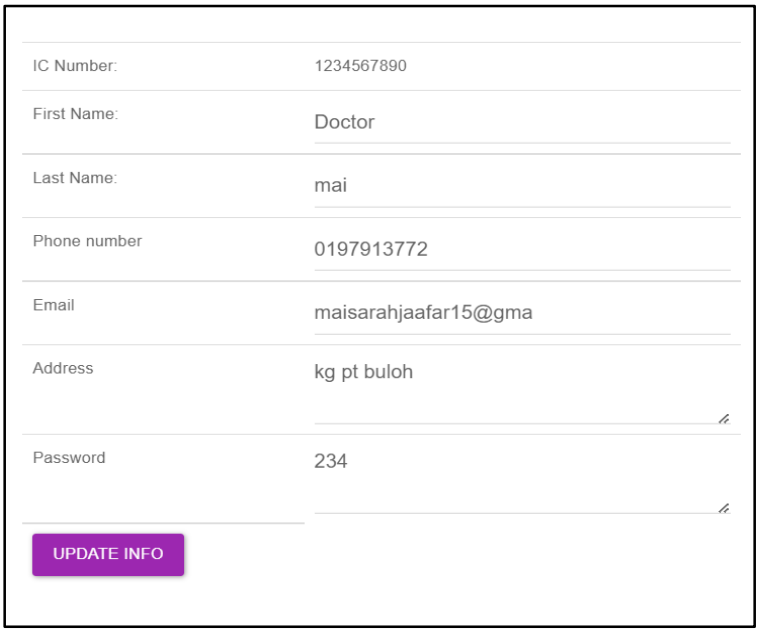

Figure 12: Update profile Interface

4.6.4 Add Doctor and Manage Schedule Interface

This module can only be reached by the admin. Admin is able to register the new doctor and able to manage all doctor's schedules. Then the related data will appear in the patient's interface during the appointment sessions. Figure 13 shows the add doctor interface and Figure 14 shows the interface for manage schedule for the doctor.

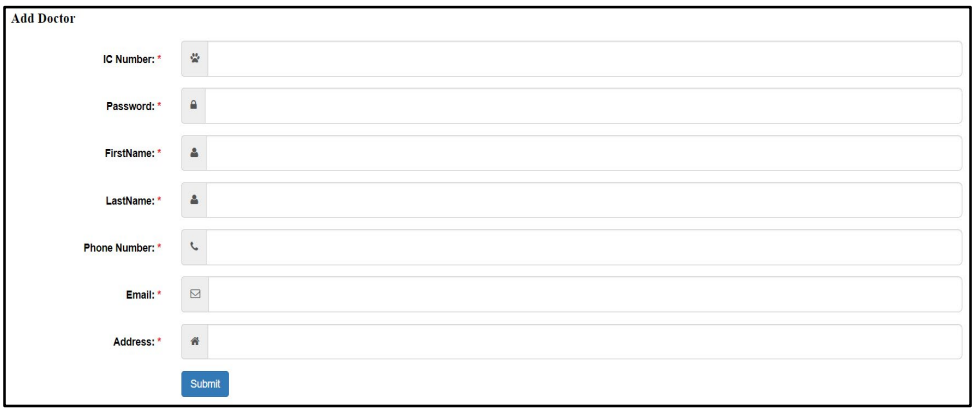

Figure 13: Add doctor interface

Figure 14: Manage schedule interface

4.7 Test Case

After the system has been completely developed, the system undergoes the testing phase to test the functionality of the system. It is used to identify if there are any bugs and errors that occurred during the testing phase. In the meantime, the scope and objectives of this purpose system can be achieved by improving the errors. Table six shows the summary of the functional testing results.

Table 4: Functional Test

No.	Function Testing	Expected Result	Result
1.	Register Function		
i.	Users leave fields empty	Error messages appear	Success
ii.	Users enter the wrong input	Error message shown	Success
iii.	Users enter the same Ic number	Error message 'Registered Ic number' will shown	Success
iv.	Users enter all the correct input	Users can proceed to login	Success
2.	Login Function		
i.	Users leave field empty	Error message shown	Success
ii.	Users enter wrong input	Error message shown	Success
iii.	If captcha not checked	Message 'Captcha not checked' will appear.	Success
iv.	Enter correct input	User can proceed to choose the date	Success
3.	Appointment booking function		
i.	Patients choose available date, doctor, and slots	User will direct to another page	Success
ii.	Patient cannot click on gray button	Patient only tick on date and slots that available.	Success
4.	Add doctor function		
i.	Only admin can add doctor	The data will store in database	Success
5.	Manage schedule		
i.	Only admin can manage doctor's schedule	The data will store in database	Success
6.	Update profile		
i.	Patient and doctor can update their profile	The update profile stored in database.	Success

4.8 User Testing

User testing is also developed to ensure that the developed system can meet the requirements and criteria that set by the target user. A total of six users that consisting of five women and one man were selected as respondents to answer the questionnaire. The google was created to distribute the questionnaire for respondents to answer the survey.

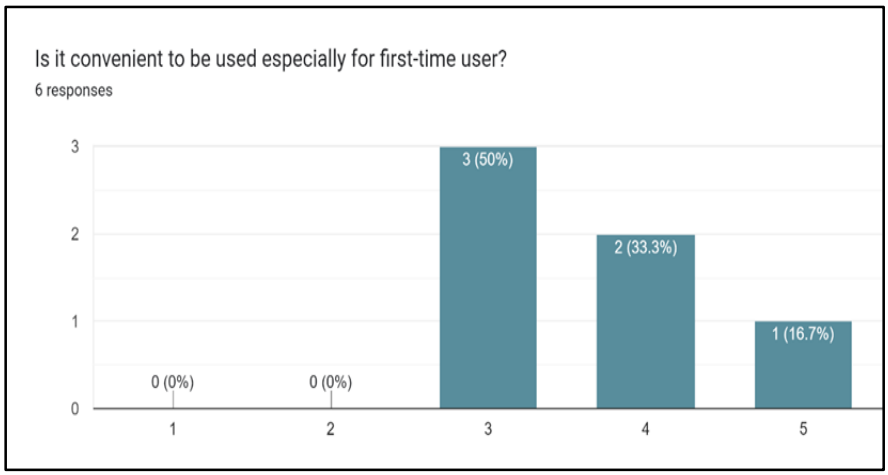

Figure 15: Percentage for user acceptance

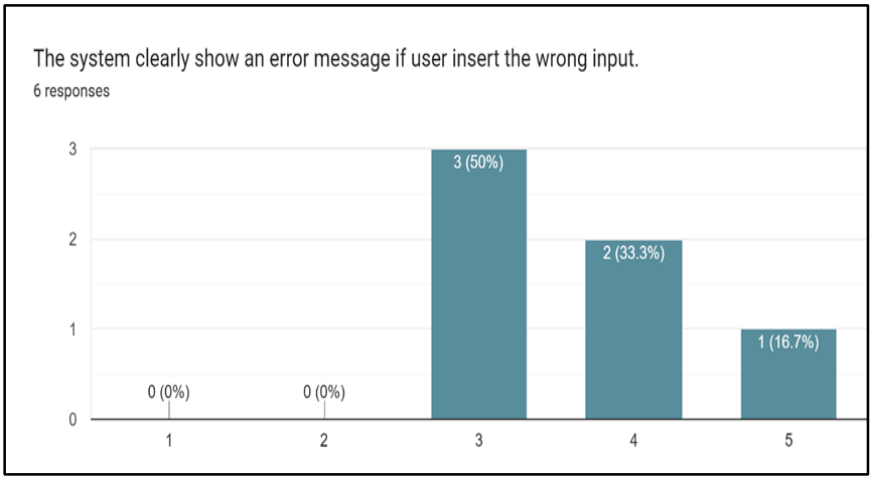

Figure 16: Percentage for user acceptance

Figure 15 shows the percentage of user satisfaction with the proposed system. Based on the survey that has been done, about 50% of the respondent choose neutral, 33.3% of the respondent choose to agree and 16.7% respondent choose to strongly agree that the system is convenient for first-time user. Figure 16 shows the percentage of user satisfaction to the system. There are 50% respondents that choose neutral, 33.3% respondents choose to agree, and 16.7 respondents choose to strongly agree that the system clearly shows an error message if user insert the wrong input.

5. Conclusion

Dr. Hannani Secure Booking Clinic System with Multi-Factor Authentication is developed to protect the authenticity of the users and the integrity of data including user's personal details, password, appointment details and schedule. Besides, multifactor authentication is implemented in this system to fulfill the security requirement for booking appointments and to allow only authorized user can access to the system.

The advantage of multifactor authentication that is implemented in this system is to reduce the risk of security breach and to protect the sensitive data in the proposed system. It is because a login page is like a first defense that needs to tighten to make sure the unauthorized cannot access the modules. Next, the proposed system uses the MD5 hashing algorithm to hash user's password into unreadable text. The disadvantage of the system is the system did not have forgotten password button. If a user forgot their password, they need to contact an admin to re-register the system again.

Therefore, the system still needs a lot of enhancements that must be upgraded for future implementation. Hence, this proposed system needs more focus on the user requirement, system requirement and security requirement to make sure all the user needed are fulfilled and the objectives can be achieved.

Acknowledgement

The authors would like to thank to Faculty of Computer Science and information Technology, Universiti Tun Hussein Onn Malaysia, lecturers, family and friends for the support and guidance during completing this project.

References

[1] W. A. Staff, "What Is an Online Booking System? (Reservation System Definition)," *Amelia WordPress Booking Plugin*, Mar. 06, 2020. https://wpamelia.com/online-booking-system/.

[2] B. S. Manoj and C. S. R. Murthy, "Transport Layer and Security Protocols for Ad Hoc Wireless Networks," *informIT database*, Jan. 21, 2005. https://www.informit.com/articles/article.aspx?p=361984&seqNum=8.

[3] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, p. 1, Jan. 2018, doi: 10.3390/cryptography2010001.

[4] A. Muhammad and R. Hikmat, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *International Journal of Computer Applications*, vol. 143, no. 4, pp. 11–17, Jun. 2016, doi: 10.5120/ijca2016910143.

[5] S. Chaudhry, F. Batool, A. Hafeez Muhammad, and A. Siddique, "Designing an Online Appointment System for Semiliterate Users," *Intelligent Automation & Soft Computing*, vol. 28, no. 2, pp. 379–395, 2021, doi: 10.32604/iasc.2021.016263.

[6] SearchSecurity, What is Authentication?, 2019. https://searchsecurity.techtarget.com/definition/authentication.

[7] Z. Davis, "Definition of password," *PCMAG*, 2021. https://www.pcmag.com/encyclopedia/term/password (accessed Dec. 30, 2021).

[8] Muhlenberg College, "Guidelines for Strong Passwords," *Muhlenberg College*, Dec. 06, 2021. https://www.muhlenberg.edu/offices/oit/about/policies_procedures/strong-passwords.html.

[9] Google Workspace Admin Help, "What is CAPTCHA?, 2021. https://support.google.com/a/answer/1217728?hl=en.

[10] What is biometric authentication? - Definition from WhatIs.com, "What is biometric authentication? - Definition from WhatIs.com," *SearchSecurity*, 2019. https://searchsecurity.techtarget.com/definition/biometric-authentication.

[11] Kaspersky, "What Is Biometrics Security," *Kaspersky.com*, 2020. https://www.kaspersky.com/resource-center/definitions/biometrics.

[12] What is RFID and How Does RFID Work? - AB&R®, 2019. https://www.abr.com/what-is-rfid-how-does-rfid-work/.

[13] SearchSecurity, "What is multifactor authentication (MFA)? - Definition from WhatIs.com,", 2019. https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA.

[14] TutorialsPoint, "SDLC Agile Model,", 2019. https://www.tutorialspoint.com/sdlc/sdlc_agile_model.htm